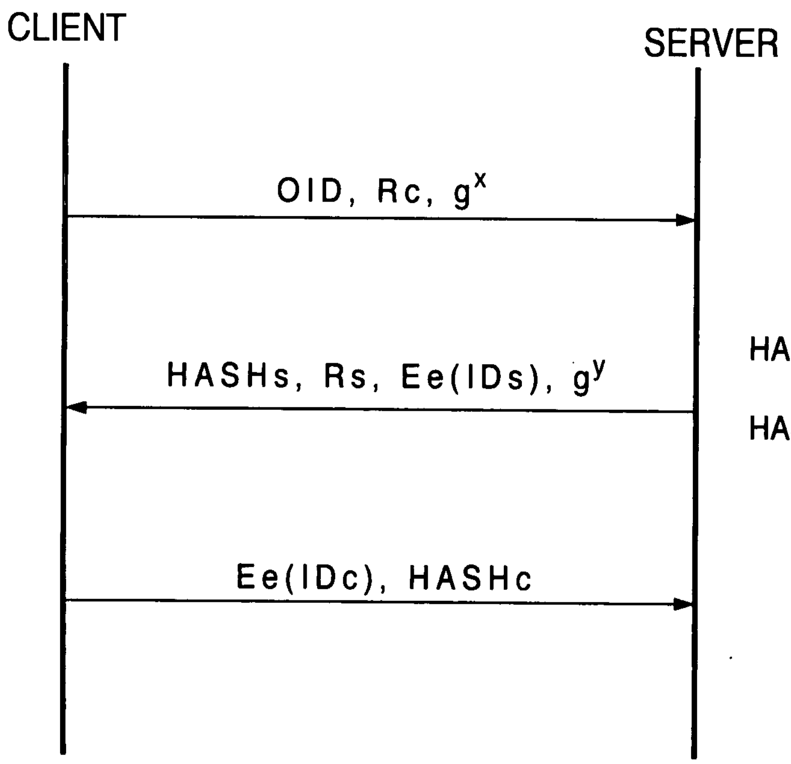
FIG.1
PRIOR ART



$e = prf\ (\text{SHARED KEY}, Rs, Rc, g^{xy})$

$HASHc = prf\ (\text{SHARED KEY}, Rs, Rc, g^{x}, g^{y}, IDc)$

$HASHs = prf\ (\text{SHARED KEY}, Rs, Rc, g^{x}, g^{y}, IDs)$

FIG.2

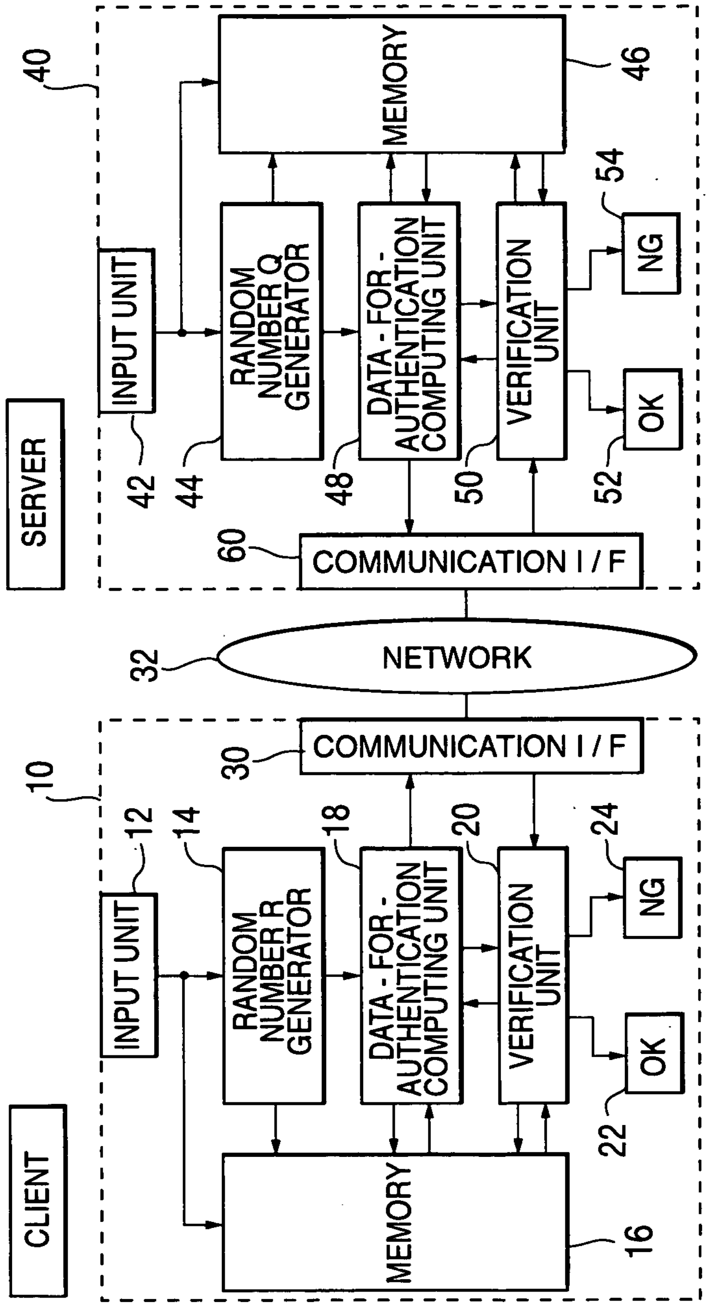

SERVER
40
INPUT UNIT
42
RANDOM NUMBER Q GENERATOR
44
MEMORY
46
DATA - FOR - AUTHENTICATION COMPUTING UNIT
48
VERIFICATION UNIT
50
OK
52
NG
54
COMMUNICATION I / F
60
NETWORK
32
COMMUNICATION I / F
30
CLIENT
10
INPUT UNIT
12
RANDOM NUMBER R GENERATOR
14
MEMORY
16
DATA - FOR - AUTHENTICATION COMPUTING UNIT
18
VERIFICATION UNIT
20
OK
22
NG
24

FIG.3

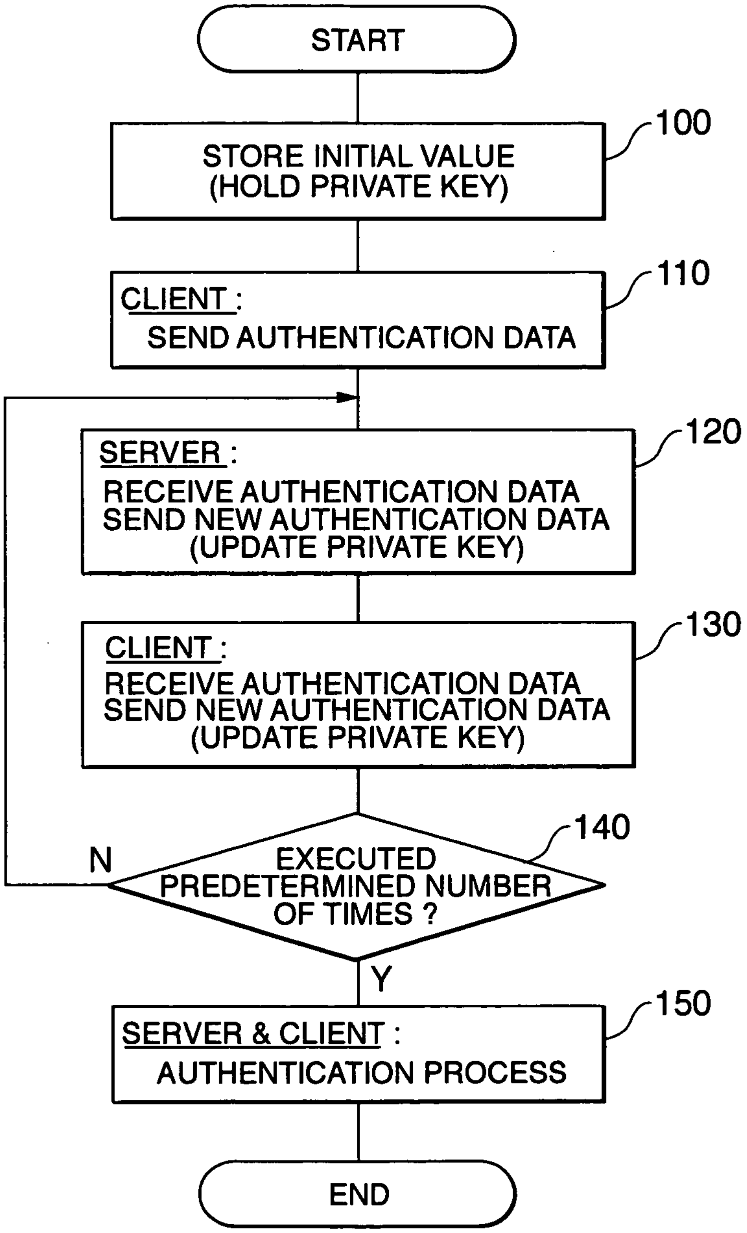

START
STORE INITIAL VALUE
(HOLD PRIVATE KEY)
100
CLIENT :
SEND AUTHENTICATION DATA
110
SERVER :
RECEIVE AUTHENTICATION DATA
SEND NEW AUTHENTICATION DATA
(UPDATE PRIVATE KEY)
120
CLIENT :
RECEIVE AUTHENTICATION DATA
SEND NEW AUTHENTICATION DATA
(UPDATE PRIVATE KEY)
130
EXECUTED
PREDETERMINED NUMBER
OF TIMES ?
140
N
Y
SERVER & CLIENT :
AUTHENTICATION PROCESS
150
END

FIG.4

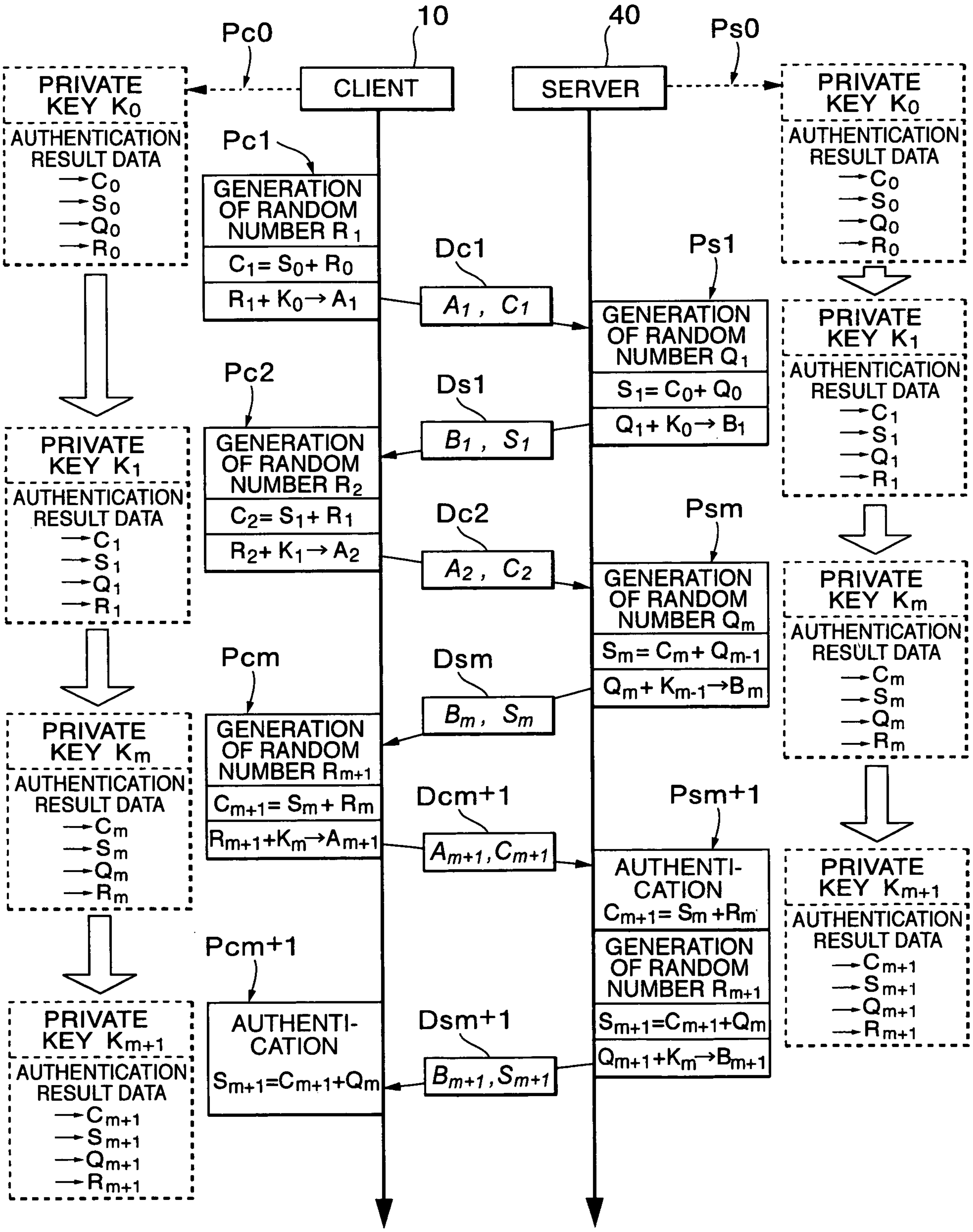

10
40
Pc0
Ps0
CLIENT
SERVER
PRIVATE KEY K_0
AUTHENTICATION RESULT DATA
→C_0
→S_0
→Q_0
→R_0
Pc1
GENERATION OF RANDOM NUMBER R_1
$C_1= S_0+ R_0$
$R_1+ K_0 \rightarrow A_1$
Dc1
A_1 , C_1
Ps1
GENERATION OF RANDOM NUMBER Q_1
$S_1= C_0+ Q_0$
$Q_1+ K_0 \rightarrow B_1$
PRIVATE KEY K_1
AUTHENTICATION RESULT DATA
→C_1
→S_1
→Q_1
→R_1
Pc2
Ds1
B_1 , S_1
GENERATION OF RANDOM NUMBER R_2
$C_2= S_1+ R_1$
$R_2+ K_1 \rightarrow A_2$
Dc2
A_2 , C_2
Psm
GENERATION OF RANDOM NUMBER Q_m
$S_m= C_m+ Q_{m-1}$
$Q_m+ K_{m-1} \rightarrow B_m$
PRIVATE KEY K_m
AUTHENTICATION RESULT DATA
→C_m
→S_m
→Q_m
→R_m
Pcm
Dsm
B_m , S_m
GENERATION OF RANDOM NUMBER R_{m+1}
$C_{m+1}= S_m+ R_m$
$R_{m+1}+K_m \rightarrow A_{m+1}$
Dcm+1
A_{m+1},C_{m+1}
Psm+1
AUTHENTI-CATION
$C_{m+1}= S_m +R_m$
GENERATION OF RANDOM NUMBER R_{m+1}
$S_{m+1}=C_{m+1}+Q_m$
$Q_{m+1}+K_m \rightarrow B_{m+1}$
PRIVATE KEY K_{m+1}
AUTHENTICATION RESULT DATA
→C_{m+1}
→S_{m+1}
→Q_{m+1}
→R_{m+1}
Pcm+1
Dsm+1
B_{m+1},S_{m+1}
AUTHENTI-CATION
$S_{m+1}=C_{m+1}+Q_m$

FIG.5

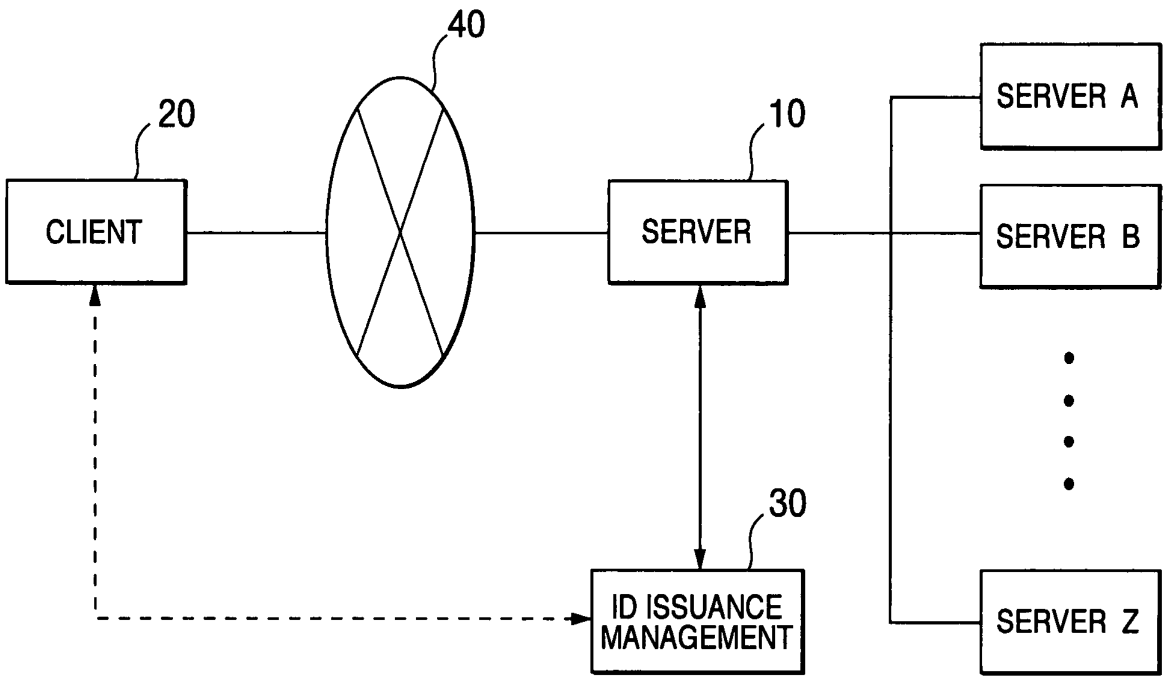

40
20
CLIENT
10
SERVER
SERVER A
SERVER B
SERVER Z
30
ID ISSUANCE MANAGEMENT

FIG.6

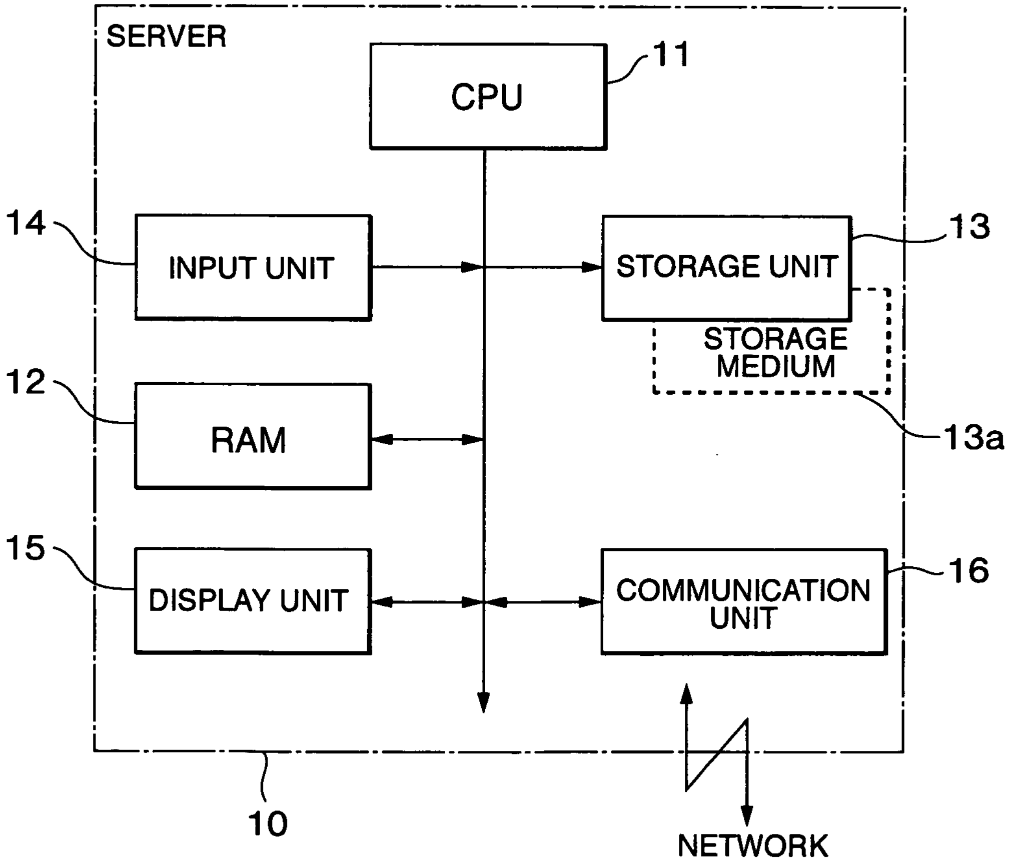

SERVER
CPU
11
14
INPUT UNIT
STORAGE UNIT
13
STORAGE MEDIUM
13a
12
RAM
15
DISPLAY UNIT
COMMUNICATION UNIT
16
10
NETWORK

FIG.7

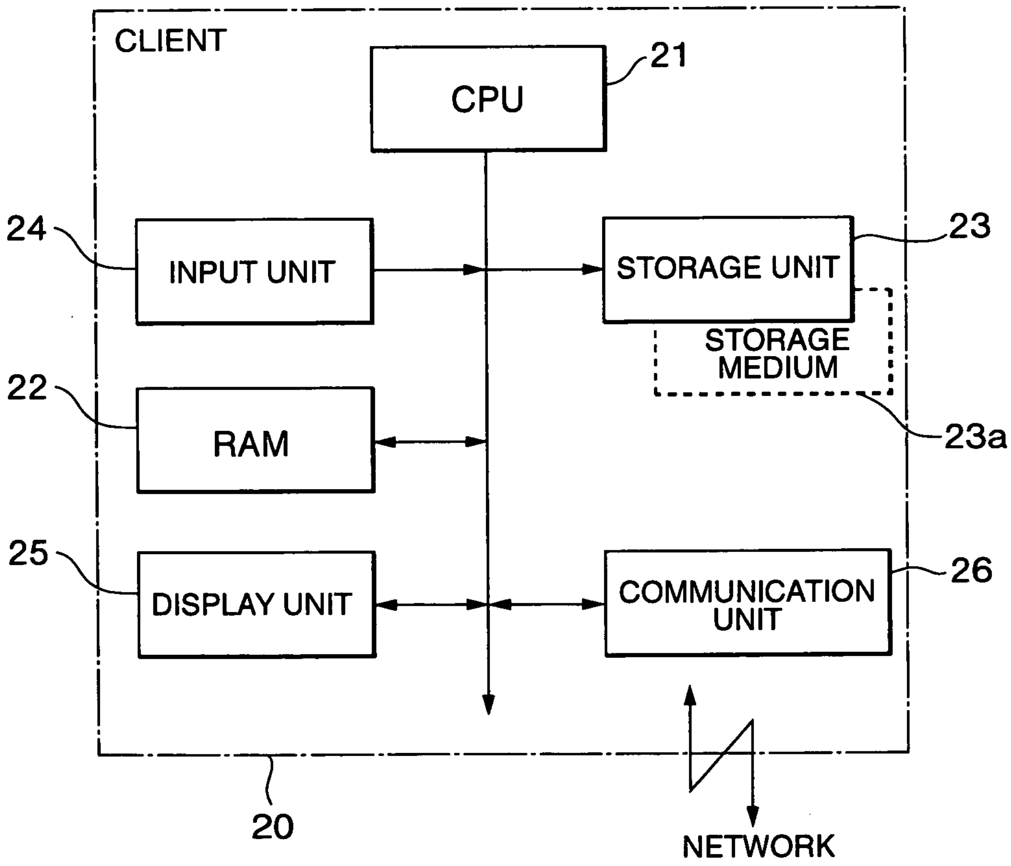

CLIENT
CPU
21
24
INPUT UNIT
STORAGE UNIT
23
STORAGE MEDIUM
23a
22
RAM
25
DISPLAY UNIT
COMMUNICATION UNIT
26
20
NETWORK

FIG.8

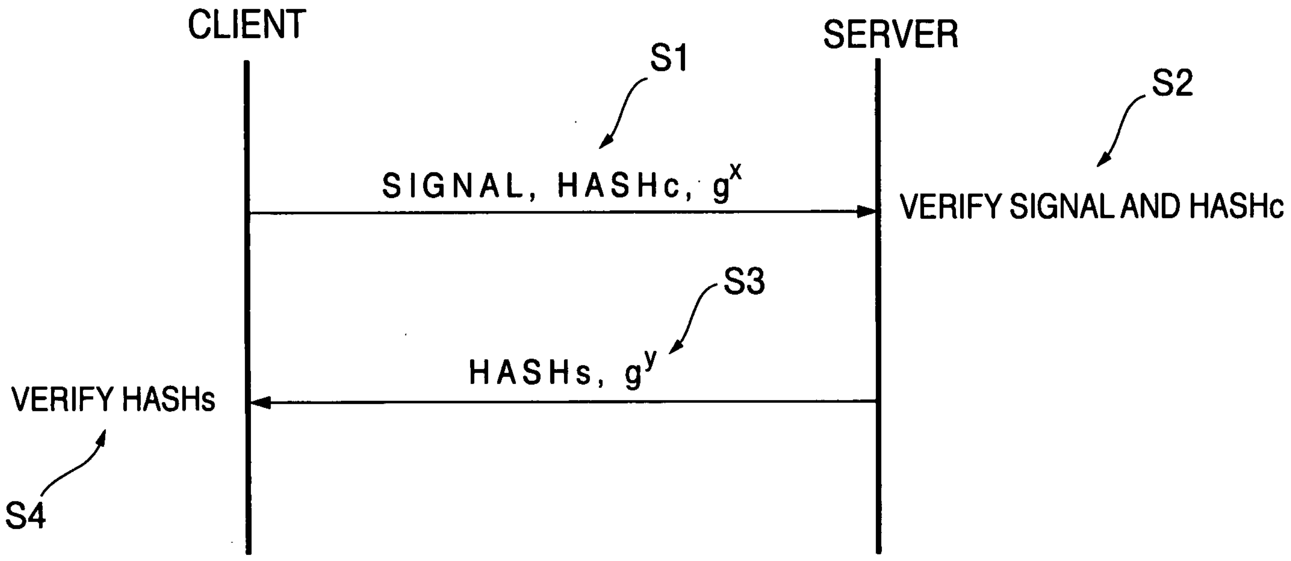

CLIENT
SERVER
S1
SIGNAL, HASHc, g^x
S2
VERIFY SIGNAL AND HASHc
S3
HASHs, g^y
VERIFY HASHs
S4

FIG.9

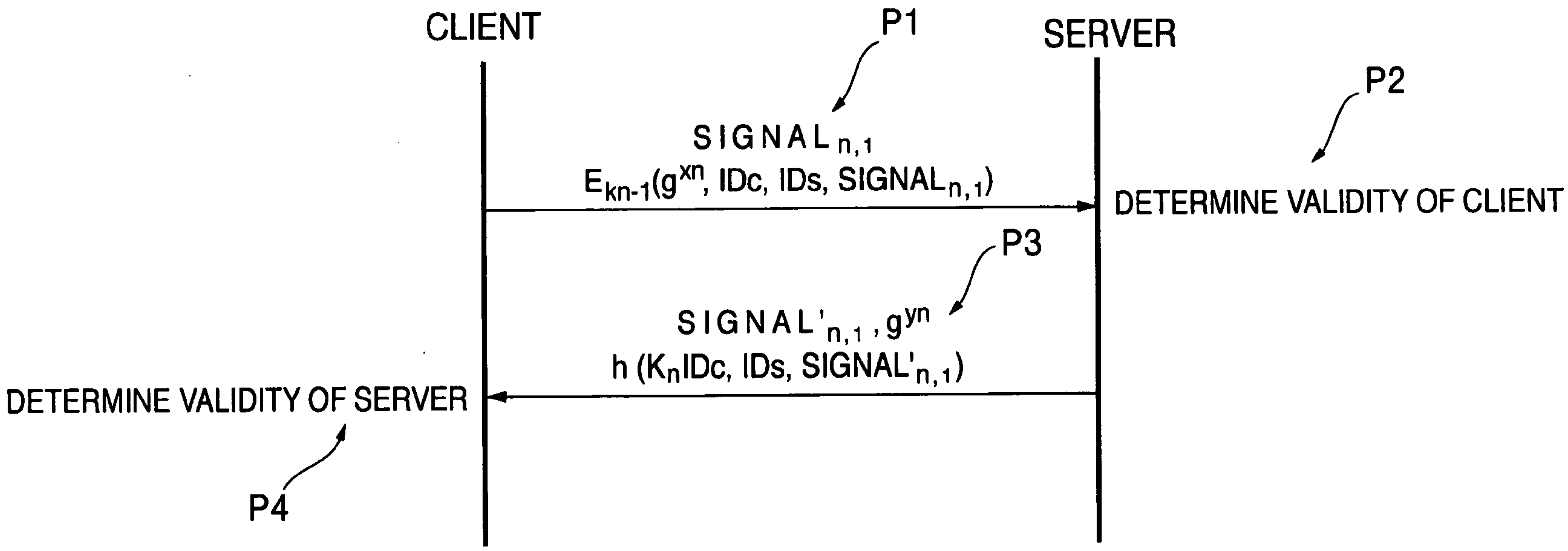

CLIENT
P1
SERVER
P2
SIGNAL$_{n,1}$
$E_{kn-1}(g^{xn}$, IDc, IDs, SIGNAL$_{n,1}$)
DETERMINE VALIDITY OF CLIENT
P3
SIGNAL'$_{n,1}$, g^{yn}
h (K_nIDc, IDs, SIGNAL'$_{n,1}$)
DETERMINE VALIDITY OF SERVER
P4

FIG.10

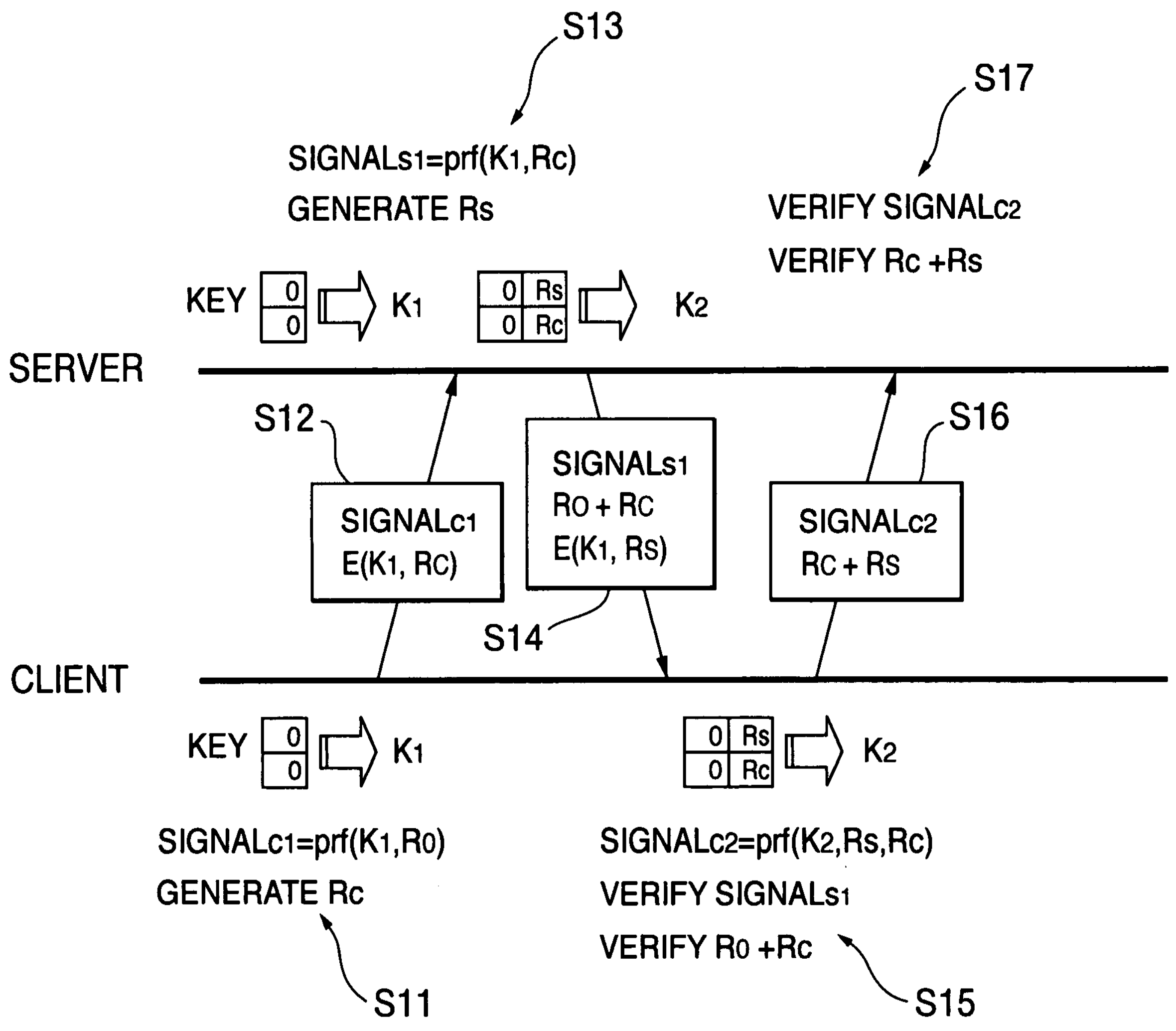

S13
SIGNALs1=prf(K1,Rc)
GENERATE Rs
S17
VERIFY SIGNALc2
VERIFY Rc +Rs
KEY
0
0
K1
0
Rs
0
Rc
K2
SERVER
S12
SIGNALc1
E(K1, RC)
SIGNALs1
RO + RC
E(K1, RS)
S14
S16
SIGNALc2
RC + RS
CLIENT
KEY
0
0
K1
0
Rs
0
Rc
K2
SIGNALc1=prf(K1,R0)
GENERATE Rc
S11
SIGNALc2=prf(K2,Rs,Rc)
VERIFY SIGNALs1
VERIFY R0 +Rc
S15

FIG.11

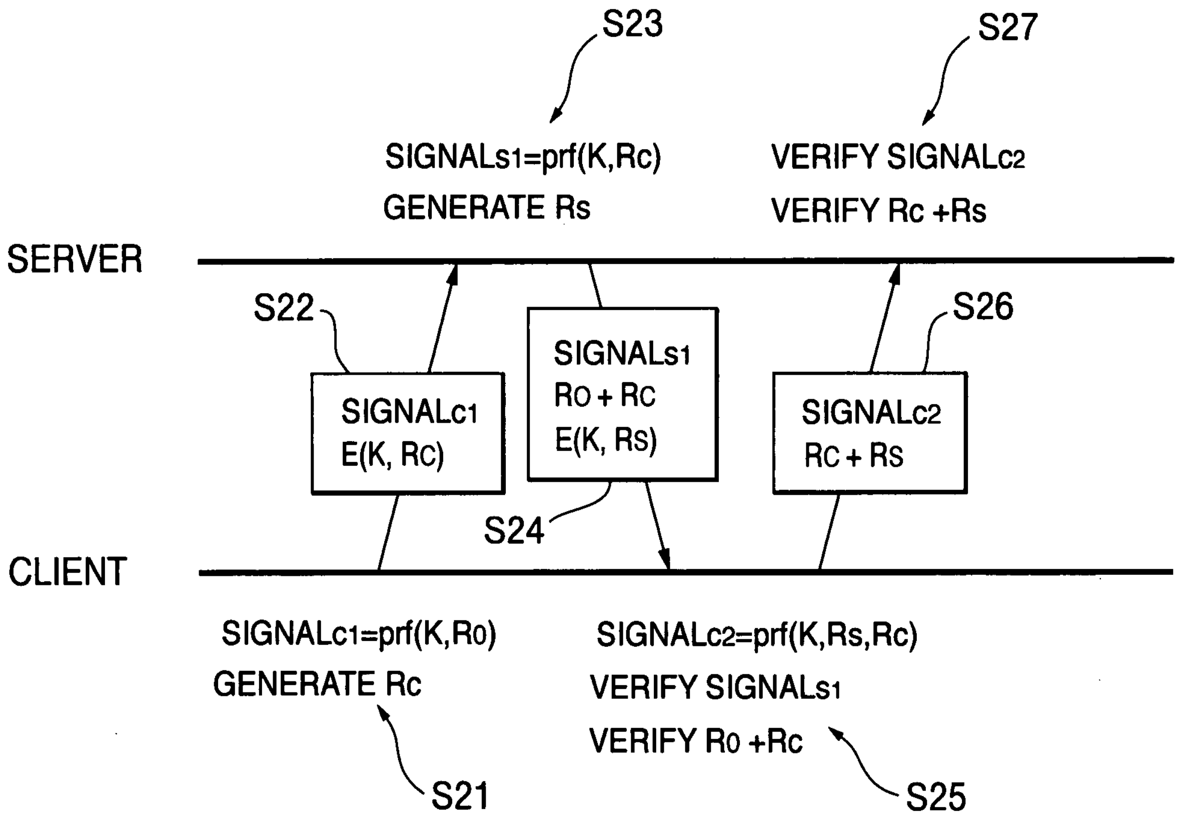

S23
S27
SIGNALs1=prf(K,Rc)
GENERATE Rs
VERIFY SIGNALc2
VERIFY Rc +Rs
SERVER
S22
S26
SIGNALc1
E(K, Rc)
SIGNALs1
Ro + Rc
E(K, Rs)
SIGNALc2
Rc + Rs
S24
CLIENT
SIGNALc1=prf(K,Ro)
GENERATE Rc
SIGNALc2=prf(K,Rs,Rc)
VERIFY SIGNALs1
VERIFY Ro +Rc
S21
S25

FIG.12

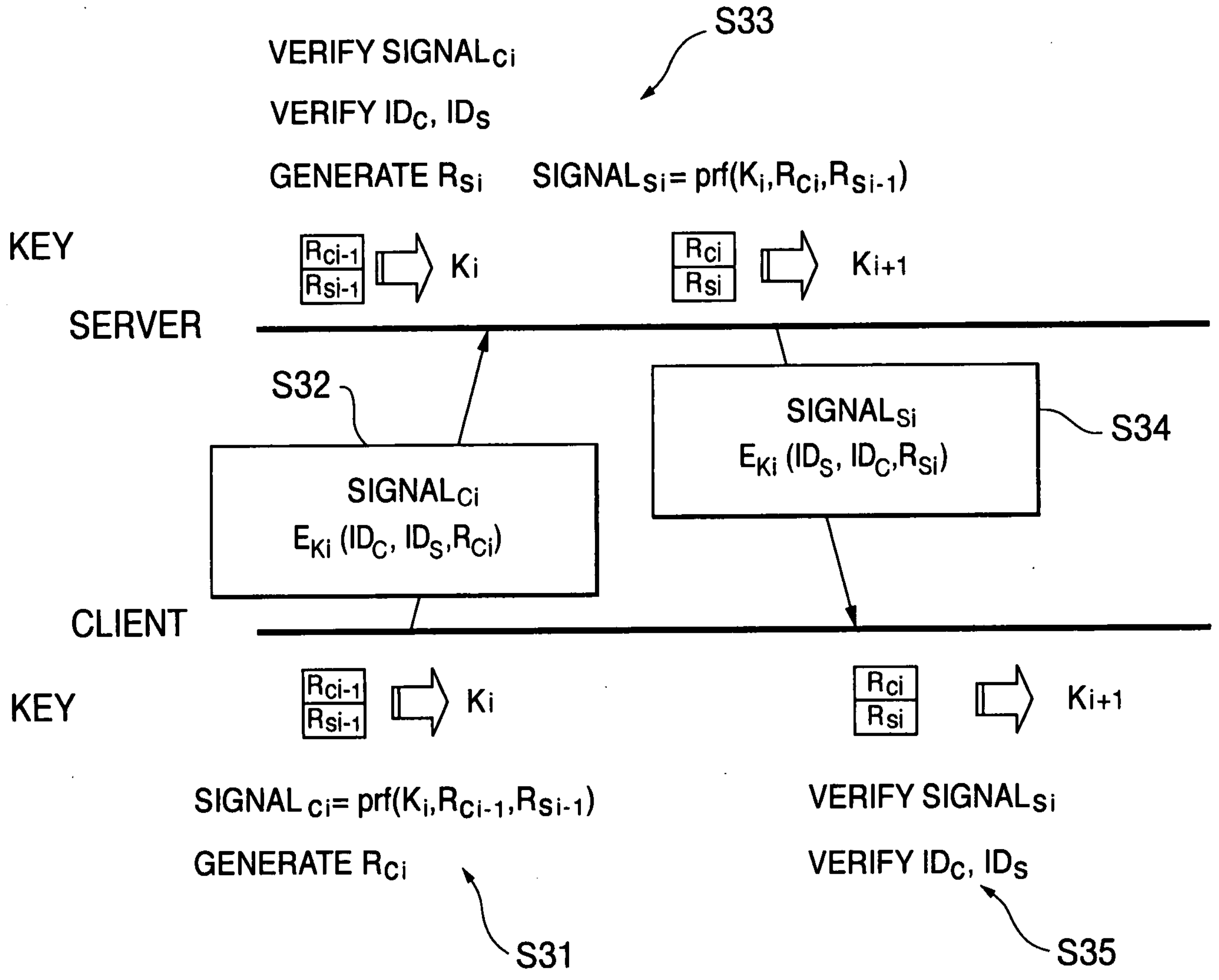
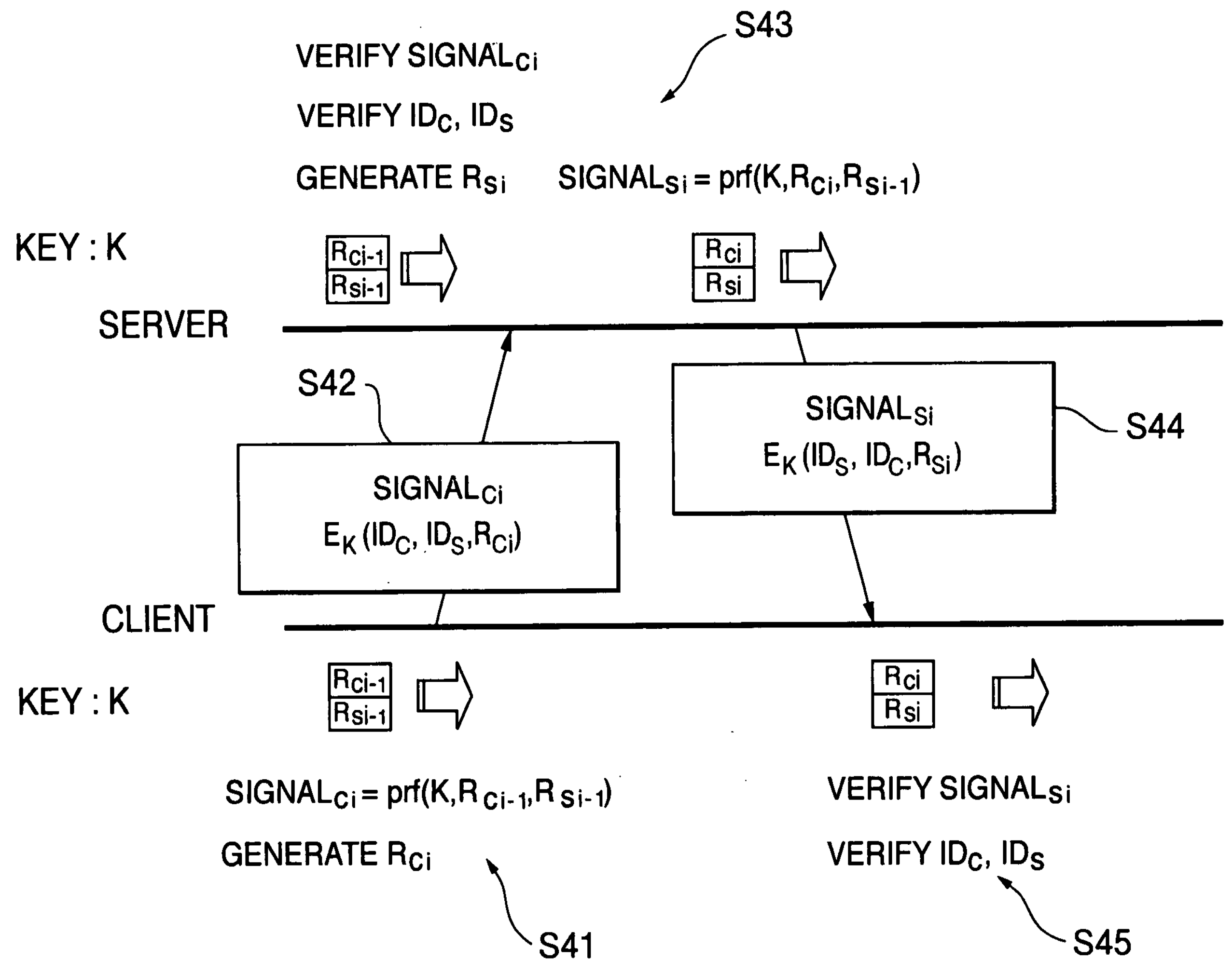

S33
VERIFY SIGNAL$_{Ci}$
VERIFY ID$_C$, ID$_S$
GENERATE R$_{Si}$
SIGNAL$_{Si}$= prf(K$_i$,R$_{Ci}$,R$_{Si-1}$)
KEY
R$_{ci-1}$
R$_{si-1}$
K$_i$
R$_{ci}$
R$_{si}$
K$_{i+1}$
SERVER
S32
SIGNAL$_{Ci}$
E$_{Ki}$ (ID$_C$, ID$_S$,R$_{Ci}$)
SIGNAL$_{Si}$
E$_{Ki}$ (ID$_S$, ID$_C$,R$_{Si}$)
S34
CLIENT
KEY
R$_{ci-1}$
R$_{si-1}$
K$_i$
R$_{ci}$
R$_{si}$
K$_{i+1}$
SIGNAL$_{ci}$= prf(K$_i$,R$_{Ci-1}$,R$_{Si-1}$)
GENERATE R$_{Ci}$
S31
VERIFY SIGNAL$_{Si}$
VERIFY ID$_C$, ID$_S$
S35

FIG.13


S43
VERIFY SIGNAL$_{Ci}$
VERIFY ID$_C$, ID$_S$
GENERATE R$_{Si}$
SIGNAL$_{Si}$ = prf(K,R$_{Ci}$,R$_{Si-1}$)
KEY : K
R$_{ci-1}$
R$_{si-1}$
R$_{ci}$
R$_{si}$
SERVER
S42
SIGNAL$_{Ci}$
E$_K$ (ID$_C$, ID$_S$,R$_{Ci}$)
SIGNAL$_{Si}$
E$_K$ (ID$_S$, ID$_C$,R$_{Si}$)
S44
CLIENT
KEY : K
R$_{ci-1}$
R$_{si-1}$
R$_{ci}$
R$_{si}$
SIGNAL$_{Ci}$ = prf(K,R$_{Ci-1}$,R$_{Si-1}$)
GENERATE R$_{Ci}$
S41
VERIFY SIGNAL$_{Si}$
VERIFY ID$_C$, ID$_S$
S45

10/518499

FIG.14

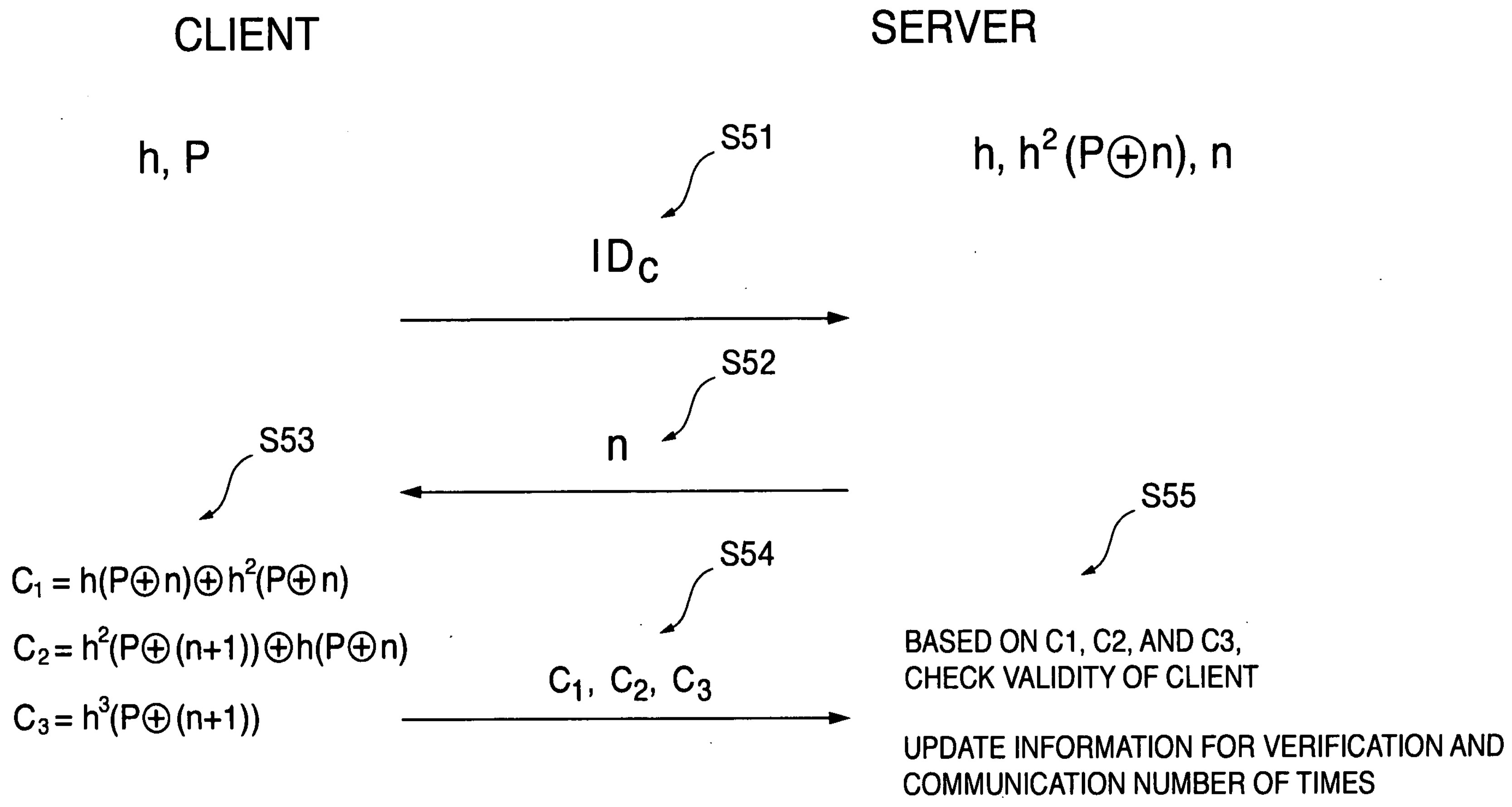

CLIENT
SERVER
h, P
h, $h^2(P \oplus n)$, n
S51
ID_C
S52
n
S53
S54
S55
$C_1 = h(P \oplus n) \oplus h^2(P \oplus n)$
$C_2 = h^2(P \oplus (n+1)) \oplus h(P \oplus n)$
$C_3 = h^3(P \oplus (n+1))$
$C_1,\ C_2,\ C_3$
BASED ON C1, C2, AND C3, CHECK VALIDITY OF CLIENT
UPDATE INFORMATION FOR VERIFICATION AND COMMUNICATION NUMBER OF TIMES

FIG.15

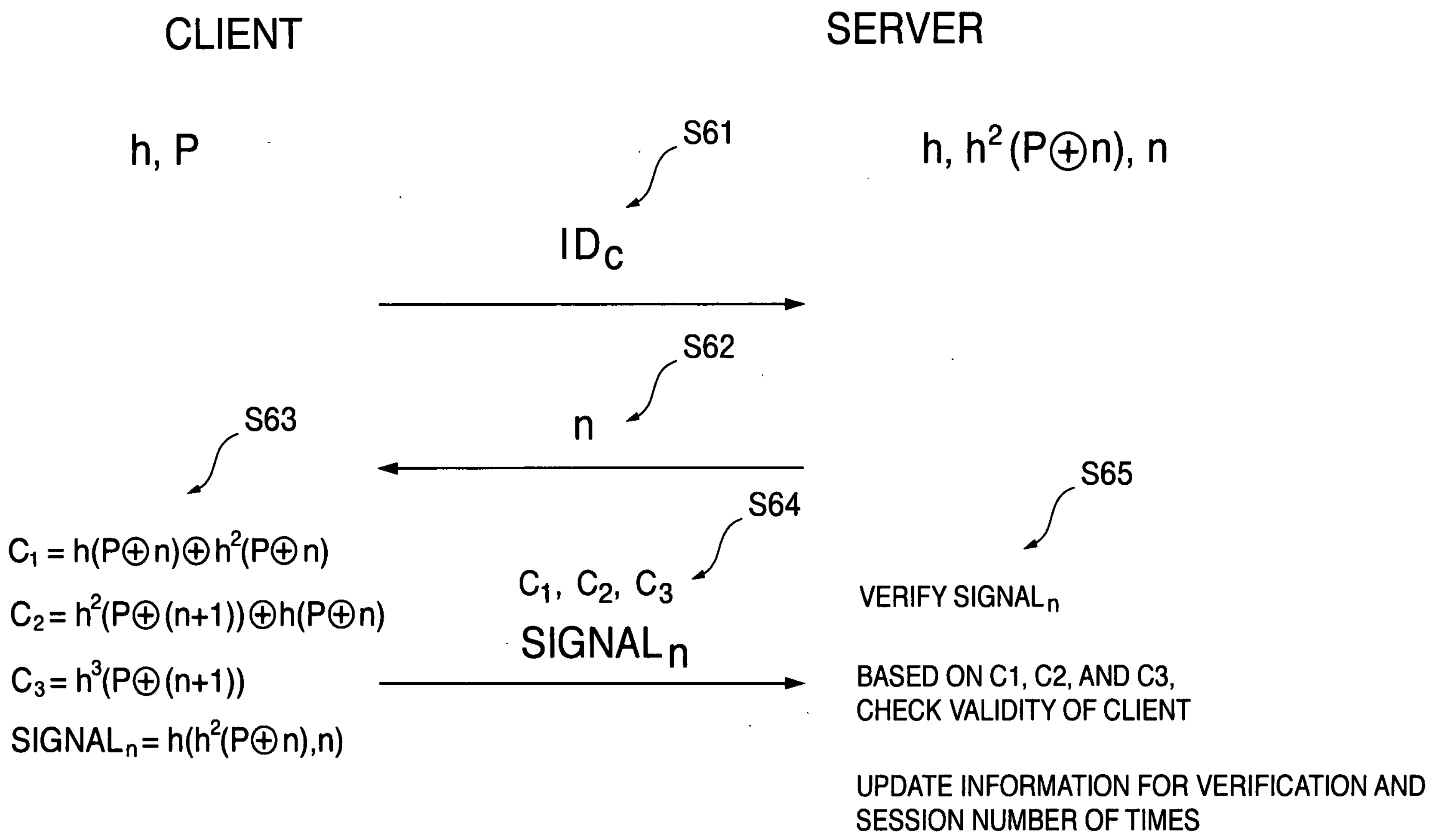
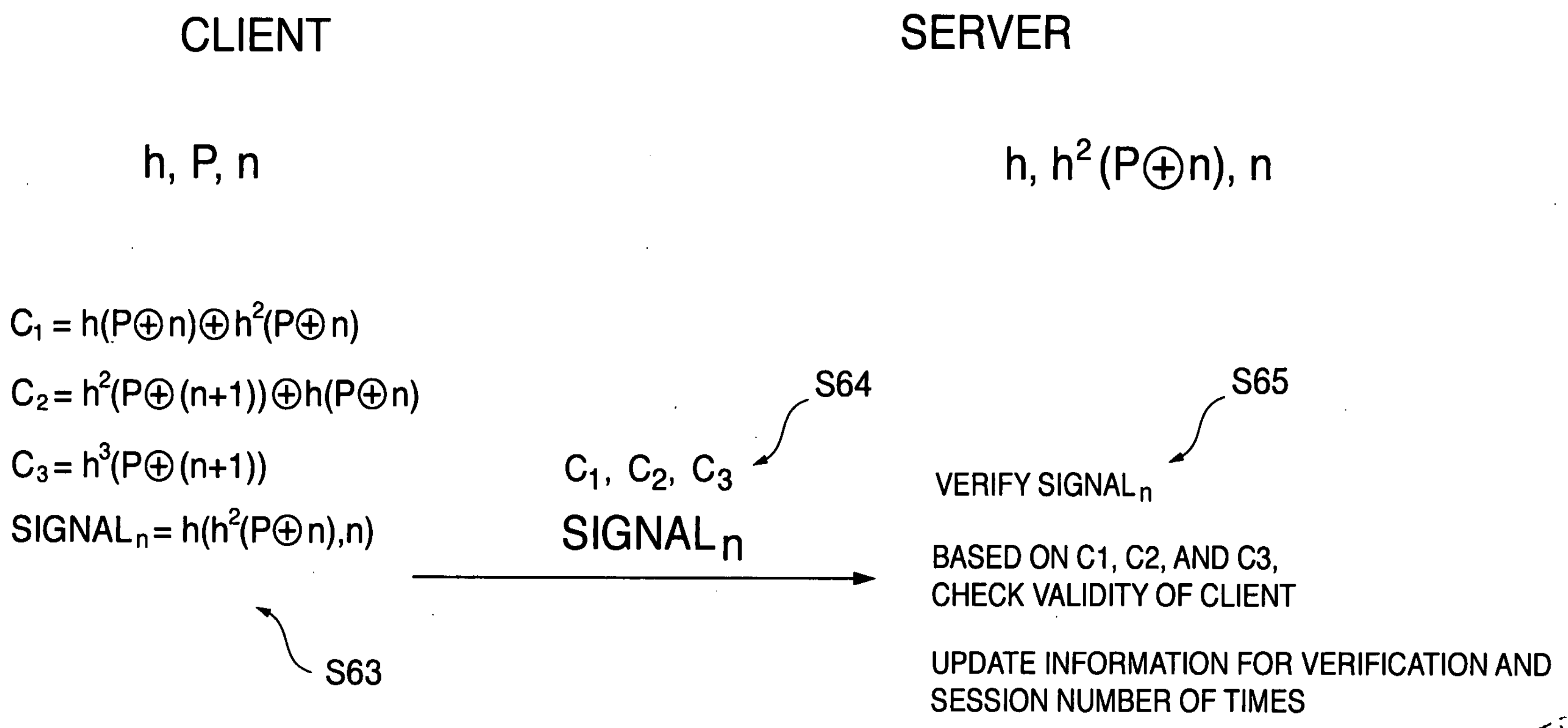

CLIENT
SERVER
h, P
S61
$h, h^2(P \oplus n), n$
ID_C
S62
n
S63
S64
S65
$C_1 = h(P \oplus n) \oplus h^2(P \oplus n)$
$C_2 = h^2(P \oplus (n+1)) \oplus h(P \oplus n)$
$C_3 = h^3(P \oplus (n+1))$
$SIGNAL_n = h(h^2(P \oplus n), n)$
C_1, C_2, C_3
$SIGNAL_n$
VERIFY $SIGNAL_n$
BASED ON C1, C2, AND C3, CHECK VALIDITY OF CLIENT
UPDATE INFORMATION FOR VERIFICATION AND SESSION NUMBER OF TIMES

FIG.16


CLIENT
SERVER
h, P, n
h, $h^2(P\oplus n)$, n
$C_1 = h(P\oplus n)\oplus h^2(P\oplus n)$
$C_2 = h^2(P\oplus(n+1))\oplus h(P\oplus n)$
$C_3 = h^3(P\oplus(n+1))$
$\mathrm{SIGNAL}_n = h(h^2(P\oplus n),n)$
S63
C_1, C_2, C_3
SIGNAL_n
S64
S65
VERIFY SIGNAL_n
BASED ON C1, C2, AND C3, CHECK VALIDITY OF CLIENT
UPDATE INFORMATION FOR VERIFICATION AND SESSION NUMBER OF TIMES